

**PCT**WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales BüroINTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>6</sup> : <b>H04L 9/00</b>	<b>A2</b>	(11) Internationale Veröffentlichungsnummer: <b>WO 99/08415</b> (43) Internationales Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)
---	-----------	--

(21) Internationales Aktenzeichen: PCT/DE98/02034  
(22) Internationales Anmeldedatum: 20. Juli 1998 (20.07.98)

(30) Prioritätsdaten:  
197 34 029.6 6. August 1997 (06.08.97) DE

(71) Anmelder (für alle Bestimmungsstaaten ausser US): SIEMENS  
AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2,  
D-80333 München (DE).

(72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): SEDLAK, Holger [DE/DE];  
Neumünster 10a, D-85658 Eggenstein (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGE-  
SELLSCHAFT; Postfach 22 16 34, D-80506 München  
(DE).

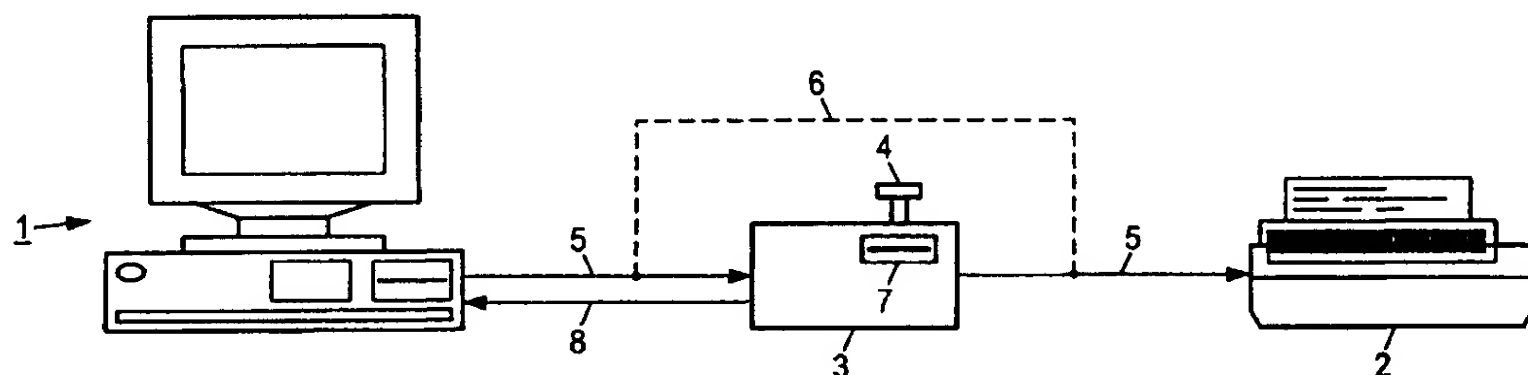
(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US,  
europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI,  
FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

**Veröffentlicht**

*Ohne internationalen Recherchenbericht und erneut zu  
veröffentlichen nach Erhalt des Berichts.*

(54) Title: SYSTEM FOR GENERATING ELECTRONIC SIGNATURES IN ABSOLUTE SECURITY

(54) Bezeichnung: EINRICHTUNG ZUM SICHEREN ERSTELLEN VON ELEKTRONISCHEN UNTERSCHRIFTEN

**(57) Abstract**

The invention concerns a system for generating electronic signatures in absolute security, comprising a system for generating data (1), a display system (2) connected thereto, and a system for reading/writing data medium (3) mounted between the data-generating system (1) and the display system (2) or parallel to the latter. Said system for reading/writing data medium (3) further comprises an activating element (4), such that the data, transmitted by the data-generating system (1) to the system for reading/writing data medium (3) for generating an electronic signature by means of an algorithm stored in a portable data medium, in particular a smart card, and a user-specific code, can be generated and/or displayed in coded form, constituting the electronic signature, only if the activating element (4) has been activated by the user.

**(57) Zusammenfassung**

Eine Einrichtung zum sicheren Erstellen von elektronischen Unterschriften weist eine Datenerstellungseinrichtung (1), eine an diese angeschlossene Anzeigeeinrichtung (2) sowie eine zwischen die Datenerstellungseinrichtung (1) und die Anzeigeeinrichtung (2) oder parallel zur Anzeigeeinrichtung (2) geschaltete Datenträger-Lese/Schreibeinrichtung (3) auf. Die Datenträger-Lese/Schreibeinrichtung (3) weist außerdem ein Betätigungselement (4) auf, so daß Daten, die zum Erzeugen einer elektronischen Unterschrift mittels eines in einem tragbaren Datenträger, insbesondere einer Chipkarte, gespeicherten Algorithmus und eines benutzerspezifischen Schlüssels von der Datenerstellungseinrichtung (1) zur Datenträger-Lese/Schreibeinrichtung (3) übertragen werden, in verschlüsselter, die elektronische Unterschrift bildender Form nur erstellt und/oder ausgegeben werden können, wenn das Betätigungselement (4) vom Benutzer betätigt wurde.

# **LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

## Beschreibung

Einrichtung zum sicheren Erstellen von elektronischen Unter-  
5 schriften

Neben der heute üblichen handschriftlichen Unterschrift soll insbesondere bei Dokumenten aber auch bei beliebigen Datensätzen eine elektronische Unterschrift möglich und rechtlich  
10 anerkannt werden. Elektronische Unterschrift bedeutet dabei, daß ein Hash-Wert der zu unterschreibenden Daten verschlüsselt wird und diese verschlüsselte Form zusammen mit den Originaldaten an den Empfänger übermittelt wird. Ein Hash-Wert ist eine durch eine Einwegfunktion verschlüsselte bzw. transformierte Form der Originaldaten. Da der Empfänger weiß, von  
15 wem die Daten stammen, kann er mit einem dem Sender zugeordneten Schlüssel, der ihm bekannt ist, die verschlüsselten Daten wieder entschlüsseln und selbst die empfangenen Originaldaten mittels der ihm ebenfalls bekannten Hash-Funktion  
20 transformieren und aus der Übereinstimmung der transformierten Originaldaten mit den entschlüsselten Daten die Korrektheit der Unterschrift ableiten und auf diese Weise die empfangenen Daten eindeutig dem genannten Empfänger zuordnen.

25 Damit die Unterschrift in hohem Maße fälschungssicher ist, müssen komplexe Algorithmen zur Verschlüsselung verwendet werden. Dies bedeutet jedoch einerseits, daß die zu verschlüsselnden Daten in einem möglichst kompakten Format vorliegen müssen, um die Verschlüsselungszeit so kurz wie möglich  
30 zu halten.

Andererseits werden jedoch bei der Erstellung der Originaldaten Programme wie beispielsweise Winword oder Excel verwendet, um eine möglichst übersichtliche und benutzerfreundliche  
35 Darstellung zu erhalten. Solche Originaldatendateien enthalten dann allerdings eine Fülle von Steuerzeichen, die oft

mehr Platz in Anspruch nehmen als die eigentlichen "Nutzdaten".

5 Einrichtungen oder Systeme zum Erzeugen elektronischer Unterschriften, das heißt also allgemein zum Verschlüsseln von Daten, weisen meist einen PC auf, der üblicherweise mit Peripheriegeräten wie einem Bildschirm, einer Tastatur und einem Drucker versehen ist.

10 Die Verschlüsselung der Daten erfolgt vorteilhafterweise mit Hilfe von Chipkarten, in denen der Verschlüsselungsalgorithmus beziehungsweise die Verschlüsselungsalgorithmen sowie der oder die dem Benutzer zugeordneten geheimen Schlüssel abgespeichert sind. Dadurch kann jeder Benutzer seinen Schlüssel  
15 und den oder die Algorithmen leicht mit sich tragen, um beliebige PCs oder auch andere Medien, wie Fax- oder Telexgeräte benutzen zu können. Es ist also zusätzlich ein Chipkartenlesegerät nötig, das jedoch bei heutigen Systemen unter der Kontrolle des Betriebssystems des PC oder eines anderen Datenerstellungs- und/oder Übertragungsmediums steht.  
20

Da die zu verschlüsselnden Daten in einem möglichst kompakten Format vorliegen müssen, werden sie also im Regelfall zum Zeitpunkt der Verschlüsselung in einem anderen Format vorlie-  
25 gen als das am Bildschirm dargestellte Format. Dies bedeutet jedoch, daß der Benutzer nie sicher sein kann, ob die zu verschlüsselnden Daten auch wirklich den Daten entsprechen, die aktuell am Bildschirm angezeigt werden. Dies um so mehr, als elektronische Unterschriften sinnvollerweise an vernetzten  
30 PCs verwendet werden, um die auf diese Weise unterschriebenen Dokumente direkt vom PC über das Netz zum Empfänger senden zu können. Dies eröffnet jedoch die Möglichkeit, daß über das Netz Dateien in den PC eingespielt werden, die eine Manipulation der zu verschlüsselnden Daten ermöglichen.

35

Auf diese Weise ist es möglich, daß zwar am Bildschirm ein Lieferauftrag für eine Firma X angezeigt wird, jedoch gesteu-

ert von dem Benutzer nicht bekannten Dateien in seinem PC,  
die ihm über das Netz zugespielt worden sind, ein Lieferauf-  
trag für die Firma Y in das Chipkartenlesegerät übermittelt  
wird, und dort mit der elektronischen Unterschrift versehen  
5 wird, um anschließend an die Firma Y geschickt zu werden.

Diese Mißbrauchsmöglichkeit wäre höchstwahrscheinlich leicht  
zu entdecken, so daß für den Auftraggeber kein wirklicher  
Schaden entstehen würde, jedoch wäre dadurch eine elektroni-  
10 sche Unterschrift im juristischen Sinne nichts wert und würde  
nicht allgemein anerkannt werden.

Die Aufgabe vorliegender Erfindung ist es daher, eine Ein-  
richtung anzugeben, bei der sichergestellt werden kann, daß  
15 die zu unterschreibenden Daten auch wirklich den vom Benutzer  
vorgesehen Daten entsprechen.

Die Aufgabe wird durch eine Einrichtung mit den Merkmalen des  
Anspruchs 1 gelöst.

20

Bei den meisten PC-Systemen ist es möglich, unterschiedlich-  
ste Peripheriegeräte von allen möglichen Herstellern anzu-  
schließen. Damit der PC mit diesen Peripheriegeräten kommuni-  
zieren kann, ist es nötig, im Betriebssystem sogenannte Trei-  
25 ber, beispielsweise Bildschirmtreiber oder Druckertreiber zu  
installieren. Diese Treiber sind Programme, die aus einem  
Standardformat ein Datenformat erstellen, das vom entspre-  
chenden Bildschirm oder Drucker gelesen werden kann. Es ist  
daher üblich, in einem PC die Möglichkeit vorzusehen, aus dem  
30 PC-eigenen Format ein solches Standardformat zu erstellen.  
Hierzu werden ebenfalls Programme verwendet, die als Fron-  
tendtreiber bezeichnet werden, während die Peripheriegerä-  
tetreiber als Backendtreiber bezeichnet werden.

35 Es gibt heutzutage noch kein einheitliches Standardformat; in  
etwa der Hälfte aller am Markt befindlichen PCs ist jedoch  
das sogenannte Post-Script-Format verfügbar. Die meisten Pe-

riperiegeräte können auch direkt mit diesem Post-Script-Format angesteuert werden.

Die Erfindung sieht nun vor, in eine Leitung zwischen dem PC  
5 und einem anzeigenden Peripheriegerät oder parallel zu dem Peripheriegerät eine zertifizierte Datenträger-Lese/ Schreibeinrichtung vorzusehen, in die einerseits die zu unterschreibenden Daten eingelesen werden und andererseits diese Daten auf dem anzeigenden Peripheriegerät, beispielsweise ei-  
10 nem Drucker oder einem Bildschirm, zur Überprüfung der Korrektheit dargestellt werden können. Das Erstellen der elektronischen Unterschrift beziehungsweise das Zurücksenden der unterschriebenen Daten an den PC erfolgt erst nach einer aktiven Bestätigung durch den Benutzer. Es ist hierbei sicher-  
15 gestellt, daß dieser Bestätigungsvorgang nicht durch den PC gesteuert erfolgen kann.

Der Vorteil dieser Einrichtung ist, daß der Benutzer am anzeigenden Peripheriegerät überprüfen kann, welche Daten in  
20 die Chipkarte zum Unterschreiben eingelesen wurden. Die Darstellung ist zwar nicht so komfortabel wie bei bekannten marktüblichen Textverarbeitungsprogrammen, jedoch ist sichergestellt, daß es dasselbe Format ist, wie bei den Daten, die in die Chipkarte eingelesen wurden, und auf diese Weise keine  
25 Manipulation durch ein weiteres im PC möglicherweise enthaltenes Programm vorgenommen werden konnte. Da die Datenträger-Lese/Schreibeinrichtung völlig autark ist, und nicht vom PC angesteuert werden kann, sondern lediglich Daten von dort erhält, ist ein Mißbrauch ausgeschlossen. Voraussetzung dafür  
30 ist allerdings, daß diese Datenträger-Lese/Schreibeinrichtung "zertifiziert" ist, das heißt von einer autorisierten Behörde überprüft und beispielsweise verplombt sein muß.

Die Datenträger-Lese/Schreibeinrichtung weist in vorteilhafter  
35 Weise einen Knopf oder ein anderes Betätigungselement auf, den der Unterzeichner drücken muß, bevor das Erstellen und/oder Absenden des unterschriebenen Dokuments oder

Schriftstücks erfolgt. Es bleibt dabei dem Unterzeichner - wie bei der bisherigen Unterschrift auch - überlassen, ob er die Korrektheit des Schriftstücks überprüfen möchte oder ob er beispielsweise durch Knopfdruck einfach nur unterschreibt. 5 Jedenfalls bedeutet das Betätigen des Betätigungselements eine eindeutige Willensäußerung.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe einer Figur näher erläutert.

10

Die Figur zeigt dabei eine vereinfachte Prinzipdarstellung der Erfindung.

Die Figur zeigt als Datenerstellungseinrichtung 1 einen Personal Computer. Im Rahmen der Erfindung sind jedoch ebenso andere Datenerstellungseinrichtungen, beispielsweise ein Faxgerät oder ein Telexgerät denkbar. Ein Faxgerät ist hier ebenfalls als Datenerstellungseinrichtung bezeichnet, da Daten in geschriebener Form in eine elektronische Form überführt werden. Die Datenerstellungseinrichtung 1 ist über Leitungen 5 mit einer peripheren Anzeigeeinrichtung 2, die im dargestellten Beispiel ein Drucker ist, verbunden. Dazwischen ist eine Datenträger-Lese/Schreibeinrichtung 3 geschaltet. Sie kann jedoch auch, wie durch eine strichlierte Leitung 6 25 angedeutet ist, parallel zur Anzeigeeinrichtung 2 geschaltet werden. Es ist außerdem denkbar, daß die Anzeigeeinrichtung 2 Bestandteil der Datenträger-Lese/Schreibeinrichtung 3 ist.

Die Datenträger-Lese/Schreibeinrichtung 3 weist einen Eingabeschlitz 7 auf, in den eine (nicht dargestellte) Chipkarte einführbar ist. Diese Chipkarte beinhaltet den Algorithmus und den geheimen Schlüssel, mittels denen Daten, die von der Datenerstellungseinrichtung 1 über die Leitung 5 zur Datenträger-Lese/Schreibeinrichtung 3 übertragen werden, verschlüsselt, das heißt zu einer elektronischen Unterschrift 35 verarbeitet werden.

Die die elektronische Unterschrift darstellenden verschlüsselten Daten werden über eine Leitung 8 zurück zur Datenerstellungseinrichtung 1 übertragen. Die Leitungen 5 und 8 können natürlich auch als bidirektionale Leitung ausgebildet  
5 sein.

Der wesentliche Bestandteil der Erfindung ist ein Betätigungselement 4, das im dargestellten Beispiel ein vom Benutzer zu drückender Knopf ausgebildet ist. Eine Erstellung und/oder  
10 Übertragung von der Datenträger-Lese/Schreibeinrichtung 3 zur Datenerstellungseinrichtung 1 der elektronischen Unterschrift erfolgt erst, nachdem der Benutzer diesen Knopf 4 gedrückt hat.

15 Da durch die erfindungsgemäße Einrichtung sichergestellt ist, daß die in der in die Datenträger-Lese/Schreibeinrichtung 3 eingeführten Chipkarte zu verschlüsselnden Daten identisch sind mit denen durch die Anzeigeeinrichtung 2 dargestellten Daten, ist die Unterschrift eindeutig und wird durch Betätigen des Knopfes 4, was auch im juristischen Sinn eine eindeu-  
20 tige Willensäußerung darstellt, getätigt. Voraussetzung für eine allgemeine Anerkennung einer solchen elektronischen Unterschrift wird allerdings sein, daß die Datenträger-Lese/Schreibeinrichtung 3 durch eine autorisierte Behörde  
25 "zertifiziert" ist, das heißt als einwandfrei geprüft und verplombt ist.



## Patentanspruch

1. Einrichtung zum sicheren Erstellen von elektronischen Un-  
5       terschriften mit
- einer Datenerstellungseinrichtung (1),
  - einer an diese angeschlossenen Anzeigeeinrichtung (2),
  - einer Datenträger-Lese/Schreibeinrichtung (3), die zwischen  
10       die Datenerstellungseinrichtung (1) und die Anzeigeeinrich-  
      tung (2) oder parallel zur Anzeigeeinrichtung (2) geschaltet  
      ist, so daß Daten, die von der Datenerstellungseinrichtung  
      (1) in die Datenträger-Lese/Schreibeinrichtung (3) über-  
      tragen werden durch die Anzeigeeinrichtung (2) darstellbar  
      sind,
  - 15   - wobei die Datenträger-Lese/Schreibeinrichtung (3) ein Betä-  
      tigungselement (4) aufweist,
  - so daß Daten, die zum Erzeugen einer elektronischen Unter-  
      schrift mittels eines in einem tragbaren Datenträger, ins-  
      besondere einer Chipkarte, gespeicherten Algorithmus und  
20       eines benutzerspezifischen Schlüssels von der Datenerstel-  
      lungseinrichtung (1) zur Datenträger-Lese/Schreibeinrich-  
      tung (3) übertragen werden, in verschlüsselter, die elek-  
      tronische Unterschrift bildender Form nur erstellt und/oder  
      ausgegeben werden können, wenn das Betätigungselement (4)  
25       vom Benutzer betätigt wurde.

1/1

